KAZEROUNI LAW GROUP, APC
Abbas Kazerounian, Esq. (SBN: 249203)
ak@kazlg.com
David J. McGlothlin, Esq. (SBN: 253265)
david@kazlg.com
Mona Amini, Esq. (SBN: 296829)
mona@kazlg.com
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

Attorneys for Plaintiff,
Aimee Levi

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

AIMEE LEVI, individually an on behalf of all others similarly situated,

Plaintiff,

vs.

ENTERTAINMENT PARTNERS, LLC; ENTERTAINMENT PARTNERS ENTERPRISES, LLC; AND ENTERTAINMENT PARTNERS SERVICES, LLC,

Defendant(s).

Case No.:

CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

1. CALIFORNIA CONSUMER PRIVACY ACT OF 2018, CAL. CIV. CODE §§ 1798.100, *et seq.*;
2. CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §§ 17200, *et. seq.*;
3. NEGLIGENCE; and
4. BREACH OF CONTRACT

JURY TRIAL DEMANDED

//

//

//

//

//

//

//

//

INTRODUCTION

Plaintiff AIMEE LEVI, individually and on behalf of all others similarly situated ("Plaintiff"), individually and on behalf of all others similarly situated (the "Class members"), by and through their attorneys, upon personal knowledge as to facts pertaining to himself and on information and belief as to all other matters, bring this class action against ENTERTAINMENT PARTNERS, LLC; ENTERTAINMENT PARTNERS ENTERPRISES, LLC; AND ENTERTAINMENT PARTNERS SERVICES, LLC (collectively "Entertainment Partners," "EP," or "Defendants"), and allege as follows:

NATURE OF THE CASE

1. This is a data breach class action against Defendants and their related entities, subsidiaries, and agents for failing to secure and safeguard the personally identifiable information ("PII") that Defendants collected and maintained from Plaintiff and the Class members. For their business purposes, Defendants collect, receive, and maintain a substantial amount of PII from individuals, like Plaintiff, in their servers and/or networks.

2. On or about August 1, 2023, data breach notice letters were issued by or on behalf of Defendants announcing that on June 30, 2023, there was a data security incident on Defendants' computer network that resulted in unauthorized access to a subset of Defendants' accounting application data which contained Plaintiff's sensitive personal information (the "Data Breach"). Defendants' notice letter confirmed that Defendants investigated and determined that Plaintiff's personal information was contained in the database files accessed, exfiltrated, or acquired by unauthorized persons in the Data Breach. Defendants' notice letter also informed Plaintiff and other similarly situated Class members that the database files impacted by the Data Breach included their PII, including name, mailing address, social security number and/or tax identification number.

3. Defendants' data breach notice letter lacked details or information necessary for Plaintiff and Class members to understand the scope and severity of the Data Breach. Further, due to this lapse in time between the Data Breach and Defendants' notice to Plaintiff and other affected individuals, unauthorized third parties who accessed and procured their PII had already been able to acquire and sell Plaintiff's and the Class members' PII on the black market or dark web, or otherwise fraudulently misuse their PII for nefarious purposes or personal gain.

4. Defendants owed Plaintiff and Class members a duty to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard the PII it collected and maintained for business purposes and stored on its servers, databases, and/or networks.

5. Defendants breached their duty by, *inter alia*, failing to implement and maintain reasonable security procedures and practices to protect PII from unauthorized access and storing and retaining Plaintiff's and Class members' personal information on inadequately protected servers, databases, and/or networks.

6. The Data Breach happened because of Defendants' inadequate cybersecurity, which caused Plaintiff's and Class members' PII to be accessed and acquired by unauthorized persons. This action seeks to remedy these failings. Plaintiff brings this action on behalf of themself individually and on behalf of all other similarly situated persons affected by the Data Breach.

VENUE AND JURISDICTION

7. This Court has subject matter of this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, and there are more than 100 members in the proposed Class, and at least one member of the Class is a citizen of a state different from Defendants.

8. This Court has personal jurisdiction over Defendants because Defendants regularly conduct business in California and maintain offices, a headquarters, and/or principal place of business in California.

9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims and damages occurred in, was directed to, and/or emanated from this District.

PARTIES

10. Plaintiff is a resident of Los Angeles County, in the State of California.

11. Plaintiff is a consumer who provided their personal information and PII to Defendants.

12. Plaintiff had their personal information and PII collected, stored, and/or maintained by Defendants.

13. Plaintiff received a data breach notice letter dated August 1, 2023 and addressed to them from Defendants entitled "Notice of Security Breach." The letter indicated that Plaintiff's PII, including their name, mailing address, social security number and/or tax identification number, was improperly accessed and acquired by unauthorized third parties through the Data Breach.

14. As a result of Defendants' failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it collected and maintained, Plaintiff's PII was accessed, exfiltrated, viewed, stolen and/or disclosed to unauthorized persons in the Data Breach.

15. Defendant Entertainment Partners, LLC is a limited liability company formed under the laws of the State of Delaware with its principal place of business and/or headquarters located at 2950 North Hollywood Way, Burbank, California 91504.

16. Defendant Entertainment Partners Enterprises, LLC is a limited liability company formed under the laws of the State of Delaware with its principal place of

business and/or headquarters located at 2950 North Hollywood Way, Burbank, California 91504.

17. Defendant Entertainment Partners Services, LLC is a limited liability company formed under the laws of the State of Delaware with its principal place of business and/or headquarters located at 2950 North Hollywood Way, Burbank, California 91504.

FACTUAL ALLEGATIONS

PII Is a Valuable Property Right that Must Be Protected

18. The California Constitution guarantees every Californian a right to privacy. And PII is a recognized valuable property right.[1] California has repeatedly recognized this property right, most recently with the passage of the California Consumer Privacy Act of 2018.

19. In a Federal Trade Commission ("FTC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored the property value attributed to PII by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[2]

20. The value of PII as a commodity is measurable. "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[3] It is so valuable to identity thieves that

---

[1] *See* John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *2 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[2] FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

[3] *See* Soma, *Corporate Privacy Trend, supra*.

once PII has been disclosed, criminals often trade it on the "cyber black-market" for several years.

21. Companies recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[4]

22. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals openly post credit card numbers, Social Security numbers, PII and other sensitive information directly on various illicit Internet websites making the information publicly available for other criminals to take and use. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list."

23. Recognizing the high value that consumers place on their PII, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share – and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their PII.[5] This business has created a new market for the sale and purchase of this valuable data.[6]

24. Consumers place a high value not only on their PII, but also on the privacy of that data. Researchers shed light on how much consumers value their data

---

[4] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

[5] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) *available at* https://www.nytimes.com/2010/07/18/business/18unboxed.html.

[6] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) *available at* https://www.wsj.com/articles/SB10001424052748703529004576 160764037920274.

privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[7]

25. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between $11.33 and $16.58 per website.[8]

26. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII Has Grave and Lasting Consequences for Victims

27. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. As more consumers rely on the internet and apps on their phone and other devices to conduct every-day transactions, data breaches are becoming increasingly more harmful.

28. Theft or breach of PII is serious. The California Attorney General recognizes that "[f]oundational" to every Californian's constitutional right to privacy is "information security: if companies collect consumers' personal data, they have a duty to secure it. An organization cannot protect people's privacy without being able to secure their data from unauthorized access."[9]

29. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government

---

[7] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* https://www.jstor.org/stable/23015560?seq=1#

[8] II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* https://ideas.repec.org/p/wpa/wuwpio/0304001.html (emphasis added).

[9] California Data Breach Report, Kamala D. Harris, Attorney General, California Department of Justice, February 2016.

benefits and incur charges and credit in a person's name.[10] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

30. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records … [and their] good name." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[11]

31. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[12] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[13]

32. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent

---

[10] *See* GAO, GAO Report 9 (2007) *available at* http:///www.gao.gov/new.items/d07737.pdf.

[11] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[12] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer, or taxpayer identification number." *Id*.

[13] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), *available at* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[14]

33. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was $150 per record.[15] Other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft – a common result of data breaches – was $298 dollars.[16] And in 2019, Javelin Strategy & Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket cost to consumers for identity theft was $375.[17]

34. A person whose PII has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."

---

[14] Brian Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying- about-identity-theft.

[15] Brook, *What's the Cost of a Data Breach in 2019*, *supra*.

[16] Norton By Symantec, 2013 Norton Report 8 (2013), *available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf.

[17] Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, *available at* https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (citing the Javelin report).

35. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[18]

36. It is within this context that Plaintiff and thousands of similar individuals must now live with the knowledge that their PII is forever in cyberspace, putting them at imminent and continuing risk of damages, and was taken by unauthorized persons willing to use the information for any number of improper purposes and scams, including making the information available for sale on the dark web and/or the black market.

Defendants' Collection of PII

37. Defendants represent that they understand the importance of protecting Plaintiff's and the Class members' personal information. For example, in its Privacy Notice, Defendants state, "We use commercially reasonable technical, organizational, and administrative measures to protect our Websites, Online Services, Payroll Services and Casting Services against unauthorized or unlawful access and against accidental loss, theft, disclosure, copying, modification, and destruction, or damage."[19]

38. Defendants' Privacy Notice represents that it collects the following categories of personal information:[20]

- Contact information, such as name, email address, postal address, and telephone number;
- Personal information and security identifiers, such as date of birth and social security numbers;
- Credentials such as a username and password;
- Demographic information, such as age and gender;
- Financial information, such as credit card, bank account, or other payment information;
- Search queries;
- Correspondence and other information that you send to us;
- Any other information identified to you at the point of collection. Information we collect automatically includes:

[18] *See* Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), *available at* https://blog.linkedin.com/2016/05/18/protecting-our-members.
[19] https://www.ep.com/legal/privacy-notice/
[20] https://www.ep.com/legal/privacy-notice/

- Log files reflecting your IP address, browser type, internet service provider, referring and exit web pages, operating system, date/time stamp, and other data reflecting your actions and activities on our Websites and Online Services;
- Location data;
- Other unique identifiers, including mobile device identification numbers;
- Information collected through cookies, web beacons, pixel tags, and other similar technologies; and
- Records of purchases made through our Websites or Online Platforms.

Information we collect from third parties includes:

- Financial information;
- Tax information; and
- Information from our clients about their current, prospective, and former Talent and Crew Members, including name address, email address, date of birth, social security number, telephone number, citizenship status, and information about their dependents and family members.

39. In the "California Residents" portion of Defendants' Privacy Notice, Defendants also state: "In the past twelve months, [they] have disclosed the following categories of personal information to third parties for business or commercial purposes:

- Personal identifiers including name, signature, address, phone number, email address, social security number, driver's license or other state identification card number, or any other personal identifier.
- Physical characteristics or description including age or gender.
- Other personal information such as national origin, marital status, or trade union affiliation.
- Financial information including bank account number, credit card number, or other financial information.
- Education and employment information including citizenship, educational background, current and prior employment, and results of criminal background checks.
- Insurance information including policy number or coverage information for health or other personal insurance.
- Internet and other network activity information including online identifiers such as IP address or device identifier, browsing history, search history, and information about interactions with websites, applications, or advertisements.
- Limited health information for lawful and legitimate purposes, including in connection with our and our clients' workplace safety initiatives, to protect EP's employees and visitors, and to comply with local, state, and federal law, regulations, ordinances, guidelines, and orders relating to COVID-19.

The Data Breach

40. On or about August 1, 2023, data breach notice letters were issued by or on behalf of Defendants announcing that on June 30, 2023, there was a data security incident on Defendants' computer network that resulted in unauthorized access to a

subset of Defendants' accounting application data which contained Plaintiff's sensitive personal information (the "Data Breach"). Defendants' notice letter confirmed that Defendants investigated and determined that Plaintiff's personal information was contained in the database files accessed, exfiltrated, or acquired by unauthorized persons in the Data Breach. Defendants' notice letter also informed Plaintiff and other similarly situated Class members that the database files impacted by the Data Breach included their PII, including name, mailing address, social security number and/or tax identification number.

41. Defendants' data breach notice letter provided little other information regarding the Data Breach itself. For instance, Defendants provided no information regarding how exactly the Data Breach occurred, how they identified Plaintiff and other affected individuals to send them notice, or how many people were affected by the Data Breach.

42. Defendants reported the Data Breach to the Office of the Maine Attorney General indicating that the Data Breach affected a total of 471,362 persons.[21]

43. As a result of the Data Breach, Plaintiff has suffered an invasion and loss of their privacy, Plaintiff has noticed unauthorized use of their PII which Plaintiff attributes to the Data Breach. Plaintiff has spent time attempting to mitigate the damages caused by the Data Breach, including monitoring Plaintiff's personal financial accounts and consumer reports, disputing unauthorized activities and transactions, filing police reports, speaking with creditors and police departments, and freezing their credit reports with credit reporting agencies, which is time that Plaintiff otherwise would have spent performing other activities or leisurely events for the enjoyment of life rather than feeling stressed, frustrated, and using their personal time trying to mitigate the impact of the Data Breach.

[21] https://apps.web.maine.gov/online/aeviewer/ME/40/6dd29d7e-9e44-4ad0-9d48-1e0bd6122ab6.shtml

44. As a result of the Data Breach, Plaintiff is, and will continue to be, at heightened risk for financial fraud, and/or other forms of identity theft, and the associated damages resulting from the Data Breach, for years to come.

Defendants Knew or Should Have Known PII Are High Risk Targets

45. Defendants knew or should have known that PII like that at issue here, is a high-risk target for identity thieves.

46. The Identity Theft Resource Center reported that the banking/credit/financial sector had the third largest number of breaches in 2018. According to the ITRC this sector suffered 135 data breaches exposing at least 1,709,013 million records in 2018.[22]

47. Prior to the Data Breach there were many reports of high-profile data breaches that should have put a company like Defendants on high alert and forced it to closely examine its own security procedures, as well as those of third parties with which it did business and gave access to its subscriber PII. Notable breaches included Capital One, which announced that in March 2019 a hacker had gained access to 100 million U.S. customer accounts and credit card applications. Similarly, in May 2019, First American Financial reported a security incident on its website that potentially exposed 885 million real estate and mortgage related documents, among others. Across industries, financial services have the second-highest cost per breached record, behind healthcare. In financial services, an average breach costs $210 per record, while a "mega breach," like Capital One's, can cost up to $388 per record.[23]

48. Anurag Kahol, CTO of Bitglass recently commented that "[g]iven that organizations in the financial services industry are entrusted with highly valuable, personally identifiable information (PII), they represent an attractive target for

---

[22] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, *available at* https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[23] Samantha Ann Schwartz, *62% of breached data came from financial services in 2019*, CioDive (Dec. 23, 2019), *available at* https://www.ciodive.com/news/62-of-breached-data-came-from-financial-services-in-2019/569592/.

cybercriminals[.]" HelpNetSecurity reports that "[h]acking and malware are leading the charge against financial services and the costs associated with breaches are growing. Financial services organizations must get a handle on data breaches and adopt a proactive security strategy if they are to properly protect data from an evolving variety of threats."[24]

49. As such, Defendants were aware that PII is at high risk of theft, and consequently should have but did not take appropriate and standard measures to protect Plaintiff's and Class members' PII against cyber-security attacks that Defendants should have anticipated and guarded against.

CLASS ACTION ALLEGATIONS

50. Pursuant to Federal Rule of Civil Procedure 23, Cal. Code Civ. Proc. § 382, and Cal. Civ. Code § 1781, Plaintiff seeks to represent and intends to seek certification of a class (the "Class") defined as:

All individuals whose PII was subjected to the Data Breach.

51. Excluded from the Class are: (1) Defendants and their respective officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

52. Certification of Plaintiff's claims for class wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

[24] HelpNetSecurity, *Hacking and malware cause 75% of all data breaches in the financial services industry* (Dec. 17, 2019), *available at* https://www.helpnetsecurity.com/2019/12/17/data-breaches-financial-services/.

53. The Class members are so numerous and geographically dispersed throughout California that joinder of all Class members would be impracticable. While the exact number of Class members is unknown, based on information and belief, the Class consists of tens of thousands of individuals, including Plaintiff and the Class members. Plaintiff therefore believe that the Class is so numerous that joinder of all members is impractical.

54. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

55. There is a well-defined community of interest in the common questions of law and fact affecting Class members. The questions of law and fact common to Class members predominate over questions affecting only individual Class members, and include without limitation:

(a) Whether Defendants had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII it collected, stored, and maintained from Plaintiff and Class members;

(b) Whether Defendants breached their duty to protect the PII of Plaintiff and each Class member; and

(c) Whether Plaintiff and each Class member are entitled to damages and other equitable relief.

56. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representatives of the Class in that Plaintiff have no interests adverse to or that conflicts with the Class Plaintiff seeks to represent. Plaintiff has retained counsel with substantial experience and success in the

prosecution of complex consumer protection and consumer privacy class actions of this nature.

57. A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class are outweighed by the costs of suit. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

58. Defendants have acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant final injunctive, including public injunctive relief, and declaratory relief with respect to the Class as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the California Consumer Privacy Act of 2018 ("CCPA")
Cal. Civ. Code §§ 1798.100, *et seq.*

59. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

60. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access. The California Legislature explained: "The unauthorized disclosure of personal

information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[25]

61. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendants failed to implement such procedures which resulted in the Data Breach.

62. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." 1798.81.5(c).

63. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

64. Plaintiff and the Class members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California

[25] California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/.

resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

65. Defendants are a "business" as defined by Civ. Code § 1798.140(c) because Defendants:

a) are a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b) "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c) do business in and is headquartered in California; and

d) have annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

66. The PII accessed and taken by unauthorized persons in the Data Breach is "personal information" as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff's and other Class members' unencrypted names, mailing addresses, social security numbers and/or tax identification numbers, among other personal information.

67. Plaintiff's PII was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including name, mailing address, social security number and/or tax identification number, at minimum, was wrongfully accessed, viewed, and/or taken by unauthorized persons in the Data Breach.

68. The Data Breach occurred as a result of Defendants' failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and Class members' PII. Defendants failed to implement reasonable security procedures to prevent an attack on its servers or systems by hackers and to prevent unauthorized access and exfiltration of Plaintiff's and Class members' PII as a result of the Data Breach.

69. On or about August 17, 2023, Plaintiff provided Defendants with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). *See* Exhibit A. If Defendants do not, or are unable to, cure the violation within 30 days, Plaintiff will amend their complaint to pursue statutory damages as permitted by Civil Code § 1798.150(a)(1)(A).

70. As a result of Defendants' failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff, individually and on behalf of the Class, seeks actual damages, equitable relief, including public injunctive relief, and declaratory relief, and any other relief as deemed appropriate by the Court.

SECOND CAUSE OF ACTION

Violation of the California Unfair Competition Law ("UCL")

Cal. Bus. & Prof. Code §§ 17200, *et seq.*

71. Plaintiff re-alleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

72. The UCL prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendants engaged in unlawful, unfair, and fraudulent practices within the meaning, and in violation of, the UCL.

73. In the course of conducting its business, Defendants committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class members' PII, and by violating the statutory and common law alleged herein, including, *inter alia*, California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100, *et seq*.) and Article I, Section 1 of the California Constitution (California's constitutional right to privacy) and Civil Code § 1798.81.5. Plaintiff and Class members reserve the right to allege other violations of law by Defendants constituting other unlawful business acts or practices. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

74. Defendants also violated the UCL by failing to promptly notify Plaintiff and Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII. If Plaintiff and Class members had been notified in an appropriate fashion, they could have taken precautions to better safeguard and protect their PII and identities.

75. Defendants' above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendants' wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendants' practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA, Article I, Section 1 of the California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available

alternatives to further Defendants' legitimate business interests other than engaging in the above-described wrongful conduct.

76. The UCL also prohibits any "fraudulent business act or practice." Defendants' above-described claims, nondisclosures and misleading statements were false, misleading, and likely to deceive the consuming public in violation of the UCL.

77. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the UCL, Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) statutory damages under the CCPA, (v) deprivation of the value of their PII for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

78. Unless restrained and enjoined, Defendants will continue to engage in the above-described wrongful conduct and more data breaches will occur. Therefore, Plaintiff individually and on behalf of the Class members, and the general public, also seeks restitution and an injunction, including public injunctive relief prohibiting Defendants from continuing such wrongful conduct, and requiring Defendants to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate cybersecurity, data security practices, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

THIRD CAUSE OF ACTION

Negligence

79. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

80. Defendants owed various duties to Plaintiff and the Class, including pursuant to the CCPA, as alleged in detail above. In addition to other duties, Defendants owed a duty to Plaintiff and other Class members in safeguarding the personal information entrusted to it by Plaintiff and the Class members. Defendants both owed duties to Plaintiff and the Class with regard to their manner of collection, transmission, sharing, and maintenance of Plaintiff's and the Class members' personal data, including PII, and were required to maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class members personal information.

81. Defendants breached their respective duties by engaging in the conduct and omissions alleged above and in violation of the CCPA and UCL, as well as each of their privacy policies as alleged above.

82. Defendants are both the actual and legal cause of Plaintiff's and the Class members' damages.

83. Plaintiff believes and thereon alleges that as a proximate result of Defendants' negligence, Plaintiff and the Class have suffered actual damages, invasion and loss of privacy, and emotional distress as described herein and above.

84. Due to the egregious violations alleged herein, Plaintiff asserts that Defendants breached their respective duties in an oppressive, malicious, despicable, gross, and wantonly negligent manner. Defendants' conscious disregard for Plaintiff's privacy rights entitles Plaintiff and the Class to recover punitive damages.

FOURTH CAUSE OF ACTION

Breach of Contract

85. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

86. Plaintiff and Class members entered into express and/or implied contracts with Defendants that included Defendants' promise to protect nonpublic personal information given to Defendants or that Defendants gathered on its own, from unauthorized disclosure.

87. Plaintiff and Class members performed their obligations under the contracts when they provided their PII to Defendants in connection with its products and/or services.

88. Defendants breached their contractual obligation to protect the nonpublic personal information Defendants gathered when Plaintiff's and the Class members' personal information was accessed and acquired by unauthorized third parties as part of the Data Breach.

89. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that (i) this action be certified as a class action, (ii) Plaintiff be designated a representative of the Class, (iii) Plaintiff's counsel be appointed as counsel for the Class. Plaintiff, individually and on behalf of the Class, further requests that upon final trial or hearing, judgment be awarded against Defendants for:

(i) actual and punitive damages to be determined by the trier of fact;

(ii) equitable relief, including restitution;

(iii) pre- and post-judgment interest at the highest legal rates applicable;

(iv) appropriate injunctive relief;

(v) attorneys' fees and litigation expenses under Code of Civil Procedure § 1021.5 and other applicable law;

(vi) costs of suit; and

(vii) such other and further relief the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial on all issues so triable.

Dated: August 17, 2023

Respectfully submitted,

KAZEROUNI LAW GROUP, APC

By: */s/ Abbas Kazerounian*

Abbas Kazerounian, Esq.
Mona Amini, Esq.
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

Attorneys for Plaintiff

EXHIBIT A

KAZEROUNI LAW GROUP, APC

245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
www.kazlg.com

August 17, 2023

VIA CERTIFIED MAIL
Entertainment Partners, LLC
Entertainment Partners Enterprises, LLC
Entertainment Partners Services, LLC
2950 N. Hollywood Way
Burbank, CA 91505

Re: Aimee Levi v. Entertainment Partners, LLC, et al.

To Whom It May Concern:

My firm represent Plaintiff Aimee Levi ("Plaintiff") and all other similarly situated consumers affected by the Data Breach described in the attached putative class action complaint against Entertainment Partners, LLC, Entertainment Partners Enterprises, LLC, and Entertainment Partners Services, LLC (collectively "Entertainment Partners" or "Defendants") arising out of, *inter alia*, Defendants' failure to provide reasonable security procedures and practices to safeguard Plaintiff's and the proposed Class members' personal information, which resulted in the unauthorized access, theft, disclosure, and procurement of their personal information by unauthorized third parties (the "Data Breach"). To our knowledge the Data Breach occurred on June 30, 2023, as specified in Defendants' data breach notification letter sent to Plaintiff and other Class members.

The full claims, including the facts and circumstances surrounding these claims are detailed in Plaintiff's Class Action Complaint, a copy of which is attached and incorporated by reference. Defendants' conduct constitutes violations of California Civil Code §§ 1798.81.5(a)(1) and 1798.150(a)(1), among other consumer protection statutes.

While this letter and the attached Complaint constitute sufficient notice of the claims asserted against Defendants, pursuant to California Civil Code 1798.150(b)(1), Plaintiff demands that, in the event a cure is possible, Defendants are hereby provided the opportunity to actually cure the noticed violations and provide Plaintiff with an express written statement within 30 days that the violations have been cured and that no further violations shall occur. A cure, if possible, requires that all the information taken has been recovered and that Plaintiff and all others impacted by the Data Breach are not at any risk of any of the information being used.

Thank you for your time and attention to this matter.

Sincerely,

s/ Abbas Kazerounian

Abbas Kazerounian, Esq.
KAZEROUNI LAW GROUP, APC
Direct Line: (800) 400-6808, Ext. 2
E-mail: ak@kazlg.com

[Enclosure]